Prospects for an Information Operations Force

By Michael O. McMahon

***Editorial Abstract:** Despite the high profile information operations have attained in joint and service-level structures, the mission largely remains homeless, without an institutional champion or advocate that generates and protects the resources necessary to accomplish it. Using current USAF efforts as a basis, McMahon argues for dedicated, fully trained and certified independent IO Force to carry out future cyber-missions.*

While it may be convenient to conclude that transformational change in our Armed Forces occurs as a result of informed insight into future threats or progressive institutional evolution, all too often change occurs as a reaction to—rather than anticipation of—seismic shifts in the national security landscape. Such changes are often hastily executed to satisfy an immediate need, and only later normalized as a new institution. As we consider the emerging threats foreign information operations and influence programs targeting the United States and its interests worldwide pose, is it possible to anticipate and implement necessary realignments to our force posture prior to a cataclysmic event that prompts hasty and poorly planned change?

A Looming Crisis

The United States is already facing a crisis in the global information space that holds our national security and foreign interests at substantial risk. We need look no farther than our own news services for examples of the predicament before us: international terrorist organizations employ web portals, bulletin boards, and e-mail communications hosted by US Internet service providers to conduct their nefarious operations ; senior military officials openly describe sophisticated, multi-year electronic intrusions into Defense Department computer networks that exfiltrate large volumes of data to foreign countries; and 24 hour satellite news services provide impressionable audiences worldwide with saturation coverage of terror, insurgency, and violence against US personnel and interests. In the midst of a global war on terror, overseas impressions of the United States are at all-time lows. Meanwhile, our Defense establishment continues to publish an ever-expanding library of policy and doctrinal statements calling for "information dominance" and "decision superiority" in the "information environment"—boldly characterized as the new battlespace of the 21st century.

Are we prepared to respond? (Defense Link)

How is it, a full decade after the Defense Department and Joint Staff began to articulate requirements for engaging these and similar threats to protect US interests in the global information space, that the Defense community continues to ask even the most basic questions concerning the posture of information operations within the overall context of US military capabilities and across the spectrum of armed conflict? In early 2001, former Assistant Secretary of Defense for International Security Affairs Dr. Ashton Carter characterized some of our most critical security priorities, to include "information warfare," as "homeless missions:" those accomplished in an ad-hoc fashion by unwieldy combinations of departments and agencies designed a half-century ago for a different world—and nowhere are the authority, resources, and accountability brought together in sharp managerial focus. Carter explains that these missions require the coordinated action of several agencies, as the problems they address do not respect neat distinctions between foreign and domestic issues, or states of war and states of peace. Carter's observations, especially with regard to information operations, have proven frustratingly durable. Despite the high profile information operations have attained in joint and service-level structures, the mission largely remains homeless; it lacks an institutional champion or advocate that focuses on the mission by generating and protecting the resources necessary to accomplish it.

Traditional military operations in the physical environment (land, sea/littoral, and air/space) have such institutions in the form of Service departments that perform the vital functions of organizing, training, and equipping combat forces. The Services also sponsor development of highly specialized weapon systems to support their combat missions. Finally, the Services have the political muscle to acquire resources, defend programs, and advocate in their own interest in the tumultuous and often hostile Federal budget process. US dominance of combat operations in the physical environment

is unsurpassed largely because of these critical Service functions. However, combat in the information environment continues to lag, because of the lack of a corresponding institutional advocate. Until the United States begins seriously to consider establishing an Information Operations Force organized as an independent Service, its efforts to engage effectively in the battlespace of the 21st century and live up to the rhetoric of its own policy documents will continue to founder. When we examine the need to prepare ourselves for combat in a new operating environment, we see that the United States has been down this road before.

A Lesson from History

The early history of the United States Air Force can provide insight into our experience with institutional change, while preparing to fight in a new combat environment. The struggle to establish an independent air service is an exhaustive tale spanning 40 years and two world wars. Although both the Department of the Army and the Navy developed air combat capabilities, it was under the Army that the air forces truly began to view themselves as an independent service. Whereas the Navy viewed naval aviation as an additional means to achieve and maintain maritime dominance, the Army-based air service developed specialized missions such as strategic bombing that were sufficiently separate from ground maneuver to spark independent thinking. Air proponents argued these missions would require substantial investment in their own theoretical and doctrinal studies, resource allocations to develop new technologies, and, ultimately, a new command structure. As long as the air service remained a component element of the Army, air advocates were convinced their interests would remain subordinated to a service ultimately dedicated to military operations on land.

It was only after World War II, when observers noted both the critical role of strategic bombing in the conflict and the simultaneous emergence of new technologies such as jet power, nuclear weapons and missile systems, that the Air Force was finally established as an independent service. It was the ultimate recognition that excellence in air and space power required the doctrinal development, mission focus, professional career sustainability, and dedicated weapon systems development that only a Service department can support. Similarly, it recognized that continued investment in strategic air capabilities by the Army would ultimately detract from its primary mission – to fight and win wars on land. By 1947, the separation was completed with the passing of the National Security Act establishing the United States Air Force as an independent Service on equal footing with the Departments of the Army and Navy.

This example can inform our discussion on the disposition of information operations capabilities today. As with air power in the early part of the 20th century, existing Service departments are making investments in information operations, largely with the view that these capabilities augment each Service's primary mission in the physical environment. Each develops its own doctrine which, in turn, drives its own disparate force development and uneven career paths for their respective officer corps and enlisted ranks. Joint force commanders frequently have little idea what information operations capabilities are truly at their disposal because of the wide disparity in levels of professional development across the service members that report for duty. Some report for duty lacking even a basic understanding of information operations concepts. This situation largely is attributable to the fact that information operations are a collateral responsibility of the existing Services, and this is reflected in the current state of doctrinal, professional, and weapon systems development.

The general disarray in the information operations community, reflected in everything from command structure, force development, and intelligence support is largely reflective of the situation of air power in the first

F-80 Shooting Star, the first operational US jet. (AviationHistory.com)

half of the 20th century; as subordinate, and ultimately collateral, responsibilities within the existing Services, the information operations community lacks a sufficient advocate to garner and focus resources, establish professional career paths from enlistee to general officer, and develop an appropriate force structure for 21st century combat. We can only hope that it will not take another world war to force necessary change.

A Roadmap to Nowhere

Are we not already engaged in a world war? Countless writers and commentators characterize the United States and its partners as being on a perpetual defensive in the global competition for opinion and influence. Consider the role of Qatar-based Al-Jazeera television in stalling Coalition operations in Fallujah in 2004, or the decisive role played by Lebanese Hizballah media and information services played in its summer 2006 war with Israel. When Usama bin Ladin and others exercise the capability to relay a strategic communication message via US news networks to the American people less than a week before they head to the presidential polls, as he did in October 2004, we should realize the global information war has already begun. Our first strategic priority should be to develop a trained and ready career force singularly dedicated to the mission of information operations. This is a primary intent of the Defense Department's *Information Operations Roadmap*. Completed in 2003 and sanitized for public release in 2006, the Roadmap documents the current shortcomings

Usama bin Ladin addresses the American people, 29 October 2004. (Associated Press)

in developing an IO career force, and makes a series of recommendations for change. Despite its good intentions, the Information Operations Roadmap is in many respects a roadmap to nowhere.

The stated goal of the study is to "transform IO into a core competency, on par with air, ground, maritime and special operations." With the exception of special operations, each of these core competencies benefit from Service institutions that develop doctrine; recruit, train and sustain a career force; and sponsor development of specialized weapon systems. Although the special operations forces do not have their own Service structure, they do benefit from several unique institutions, such as a dedicated Combatant Command with independent acquisition and training authority, which ensures mission readiness. It is difficult to envision bringing information operations to the same level of proficiency as these competencies while lacking the same structures and institutions that support and sustain them.

The Roadmap aggregates 15 topic areas as designated in the *2004 Defense Planning Guidance* into 5 major areas for reform: Policies and Procedural Controls; Command and Control and Supporting Organizations; Trained, Educated and Ready Career Force; Analytic Support; and Enhanced Core Capabilities. In each corresponding "Current Situation" section, the study rightly and accurately captures the disarray in the information operations community. However, many of the recommendations are at best half-measures when we fully consider the scope of the problem and the nature of the threat facing the nation. For example, under "Policies and Procedural Controls", the study finds "there is not a consensus on how to define IO or its contribution to warfighting", and later "the Department cannot currently identify what is spent on IO or even on specific core capabilities". These concerns speak to the general disorder at the very foundations of the information operations community, and reveal the need for a fully-empowered advocate to establish these definitions and doctrines, and account for the means by which a national force capability will be trained, equipped and organized to carry them out. These concerns will not be remedied by yet another generation of Departmental or Joint Staff policy documents; rather, they would best be addressed by a Service-level institution that is empowered to act, can speak with authority, and account for itself.

Perhaps the most important section of the Roadmap for this discussion is its third major area: A Trained and Ready Career Force. Again, the study provides accurate and illuminating descriptions of the current state of affairs in the information operations workforce: "Service constructs of IO produce a varying work force. The five capabilities of IO are not universally defined, understood or applied across the Service Departments. As a result, each Service develops specialists in those disciplines that meet Service-specific requirements… the complexity and technological growth in EW, PSYOP and CNO tend to isolate the specialists who practice these disciplines from one another… there if often little application or awareness of the relationships of one core capability to the others… retention of personnel possessing these key skill sets may be a challenge… officers assigned to Combatant Commands lack necessary operational IO planning experience and must depend upon on-the-job training—the military population lacks an understanding of IO as well."

These observations speak directly to the problem of each Service attempting to build an information operations cadre in the context of preparing for combat operations within its primary physical domain (land, sea/littoral, air/space). Each service maintains independent doctrine, training and education, and work force development programs for information operations which leave the joint force commander in the unenviable position of attempting to sort out each service members' skills, capabilities and mindset even before operational planning can begin. These points highlight the lack of a common military culture in the field of information operations; a culture created by officers and enlisted personnel forming collegial bonds from the beginning of their careers in their respective training and education programs that clearly inculcate mission, doctrine, and capability from the outset. These are the types of bonds formed not at joint commands, rather within Services.

Although the Roadmap does not address the idea of creating an independent Service for information operations, it does suggest "it may be necessary to consider making IO a dedicated military occupation specialty or career field." Although this may improve career force development within the respective services, it will not remedy ongoing concerns that the Services themselves cannot provide comparably prepared officer and enlisted specialists to a joint force commander. This recommendation is a well-intentioned half-measure.

Ultimately, the Roadmap fails to address the structural problem of information operations as a collateral function of the Services. Despite the steady support provided by the Services, it is unlikely they will ever devote the resources and personnel necessary to move information operations to the place it needs to be for combat in the 21st century at the expense of their primary missions.

Sovereign Options

Although each Service continues to make investment in information operations, the United States Air Force clearly is leading the way with a wide range of structural changes designed to elevate information operations within

its range of combat capabilities. As captured in its December 2005 mission statement, the Air Force is now posturing itself to "…deliver sovereign options for the defense of the United States of America and its global interests – to fly and fight in air, space, and cyberspace" . In effect, the Air Force will attempt to fully support combat superiority fully in two entirely separate operational domains; the physical (air/space) and the informational (cyberspace).

Examples of the Air Force's investment in information operations include unique doctrinal developments, command structures, and combat units. Air Force doctrine builds a seamless link between combat superiority in air, space, and cyberspace largely through evolutionary developments in its intelligence and airborne reconnaissance capabilities. A brief review of the history of the 67th Network Warfare Wing shows its lineage in the field of airborne reconnaissance and technical intelligence collection. These capabilities merged in August 2000 with the establishment of the 67th Information Operations Wing, a first-of-its-kind unit that supported the emerging concepts of "battlespace awareness" and "information superiority" through the execution of both offensive and defensive information operations. Today, the 67th Network Warfare Wing demonstrates its commitment to the discipline of information operations by organizing, training, and equipping an organic fighting force to carry out these missions.

The Air Force is also restructuring its intelligence and reconnaissance organizations that will support the further development of information operations capabilities. In May 2007, Air Force officials announced the establishment of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, a centralized organization that "underscores the nature of ISR as an Air Force-wide enterprise." This ISR agency will also be postured to support a reorganized 8th Air Force under the title Air Force Cyberspace Command. Significantly, Air Force Secretary Michael W. Wynne has stated that the Air Force is working to "develop educational plans and career paths for those Airmen that will work within the new command" (emphasis added). In terms of doctrine, structure, and career force development, the Air Force clearly is making substantial investments in the field of information operations.

But where will it all lead? Is it possible for the Air Force to sustain the necessary commitments to information operations without compromising its initial missions of air and space superiority? As the Air Force continues to expand its organic information operations capabilities, it likely will find itself in the same position as the Army did in the first half of the 20th century, with a burgeoning component force yearning for the independence it rightly requires to fully develop doctrine, career paths, and combat capabilities. It would be ironic, indeed, were the Air Force to cling to information operations as the Army did with the air service for so long. By taking the additional step of linking its doctrinal foundations closely across the physical and information domains, the Air Force may make the inevitable separation all the more difficult. Already, some observers note the Cyberspace Command likely will build information operations capabilities that will extend well beyond the Air Force, and the successful concentration of funding and capabilities could promote Cyberspace Command as a Defense-wide center for cyberwarfare operations. In time, Cyberspace Command potentially could develop into a joint structure, with independent authorities for training and procurement such as US Special Operations Command enjoys today.

67th Network Warfare Wing Airmen in action. (US Air Force)

A Way Forward

Although each of the Services is investing in information operations capabilities, this discussion has focused on the Air Force, because it is proceeding with substantial investments and institutional changes that a future 'IO Service' ultimately will draw upon. However, all of the Services ultimately would contribute personnel and resources at the time of its establishment. The question facing defense planners today should be one of evolution or revolution. An evolutionary approach would entail an extended nurturing period, not unlike the early air service components under the Army. Under this model, defense planners would carefully monitor the development of a national information operations capability within the existing Services until two specific break-points: 1) information operations reaches a level of maturity, as characterized by doctrinal sophistication, professional development, and overall combat capability that exhibit the ability to stand on its own, and 2) the existing Services' continued investment in information operations begins to compromise their primary missions in the physical domain. In our historical example, the air service became an independent Air Force only after its massive expansion during the Second World War. Will we need the experience of a future "Information War One" to prompt a similar development?

Some may argue that Information War One has already begun; therefore, the mandate already exists for a revolutionary approach that would entail the immediate consolidation of existing information operations capabilities into an

Information Operations Force. Although this option may appear attractive to advocates of structured career paths and professional development, other aspects such as doctrine, strategy, integration within joint command structures, and operationalization of emerging capabilities require additional work. Clearly, the complete package of doctrine, professional development, and weapons systems lack the maturity required for information operations to make an immediate break from parent services at this time. Given these options, the evolutionary approach is the better course. Because substantial progress has already been made, we should hope for a maturation period of shorter than 40 years.

What will warfare look like in the 21st century? Many feel major armed conflict between states has become anachronistic and future warfare will consist primarily of intrastate affairs focused on issues of national, cultural or religious identity, rather than on the grand ambitions of major powers. Others suggest that major interstate warfare is only on "temporary hold" because of this short, transitory period in which the United States faces no real challenger to its conventional combat capabilities – a situation that can certainly change later this century, as emerging or resurgent conventional powers develop their force structures to sufficient parity with the United States. In either scenario, it is virtually impossible to envision a future conflict in which comprehensive battlespace awareness, strategic messaging, sophisticated employment of international media, cyber operations, and effective opinion shaping will not play critical roles. Combat in the 21st century must be engaged, sustained, and won in both the physical and informational domains.

Are we best postured for 21st century combat? (Lockheed Martin)

Our adversaries have already engaged us in the information domain and our responses have been marked largely by disarray. Information operations call for engaging the adversary in an entirely new combat environment - one that requires a trained cadre of military experts. They would share a common professional culture and enjoy the confidence of a dedicated institution that would provide them with the resources and weapon systems to allow them to excel in combat. To offer our nascent information warriors anything less is to undercut their potential and place our own national interests at serious risk.